

# INFORMATION SECURITY

## IMPACTING SECURITIES VALUATIONS

---

***A. Marshall Acuff, Jr. CFA  
Salomon Smith Barney, Incorporated***

### **INFORMATION TECHNOLOGY AND THE INTERNET CHANGING THE FACE OF BUSINESS**

The Internet revolution coupled with the already ubiquitous nature of information technology has forever changed the way businesses will do business in the future. It has enabled enormous productivity enhancements across industries, created tremendous new profit making opportunities, and has accelerated the globalization of businesses and markets around the world.

Unfortunately, the tremendous prosperity that the Internet and information technologies have fostered does not come without a price. The power of the Internet is derived from the premise that an interconnected global marketplace enables tremendous cost savings, productivity enhancements and opens the doors to new markets for many businesses.

However, the open access nature of the Internet, which facilitates a freer exchange of ideas, goods and services also, presents the largest obstacle, in the way of security, to its continued success. In order to maximize the potential of the Internet and information systems within companies, the need to be part of the “network” is critical. However, being on the “network” means that companies and their information systems are exposed to attacks in cyberspace. Now, managers must not only be concerned about internal systems security, they must be ever vigilant in regards to who they are transacting business with over the web.

Even seemingly legitimate interactions over the Internet have the potential to be Trojan Horses as sophisticated criminals and hackers push the limits of technology. While we believe that the pervasiveness of the Internet will only increase, the issue of security of both the physical infrastructure as well as the trillions of bytes of information that float around in cyberspace,

should be, is, and will continue to be of paramount importance to businesses, investors, government and the public at large.

### **INFORMATION TECHNOLOGY: SCOPE AND SCALE**

While we are confident that most businesses and their managements appreciate the gravity of information technology security, we believe this is an opportune moment to focus the attention of the investment and business communities on this issue.

With Internet related revenues expected to grow at a compounded annual growth rate (CAGR) of 98% to **\$1.3 trillion by 2003**, up from \$43 billion in 1998 according to Forrester Research, and information technology spending running at 4% of total GDP (\$320 billion) up from less than one half of one percent thirty years ago, the stakes are high.

Competitive market pressures almost assure that the scope and scale of the Internet will continue to expand. In our opinion, companies have only two choices in regards to the Internet freight train: they must either hop onboard and embrace the potential which the Internet has to offer or else be left standing at the station.

Granted that with this new opportunity comes new challenges and new risks. In the past, industry could be much more reactive to changes within their environment. The internet age forces companies and managers to be much more proactive both in terms of implementing new products and applications but also in their risk assessment and risk profile as a result of doing business in a wired world.

Business must anticipate how their systems and information can be manipulated, corrupted or misappropriated, used against them or for someone else's benefit, and then determine how to combat those risks and insure that they do not come to fruition.

### **THREATS AND CONSEQUENCES: INFORMATION WARFARE**

The adage that information is power is appropriate in the context of what we are talking about today. Both in the public and private sector, information about your customers and your competitors is invaluable. It can be used to predict customer demand or develop and market new products and services. However, in the hands of individuals with malicious intent, information can be used as a tool for fraud,

deception or destruction.

There are obviously varying degrees of threats within cyberspace ranging from the teenage hacker to the professional criminal. While the average hacker may be more of a nuisance than anything else, they have the potential to be economically disruptive or physically hazardous.

Recent examples include such well-known companies as Amazon.com, Ebay and Yahoo whom all fell victim to cyberattacks. In each case, the company was economically impacted due to loss of service, which effectively eliminated their ability to transact business for a period of time. While, the incidents were relatively short lived, they exposed to the world, the vulnerability of anyone who transacts business on the web. For individuals already wary of cyberspace, it reinforced their suspicion and for the rest of us, it took away a little piece of mind.

A less well known incident in March of 1997 involving a juvenile using a basic PC was able to disable a telephone switch that resulted in service outages to the local community, including emergency services and a small airport tower. Fortunately, no one was directly

harmed, however, the potential damage is obvious and the liability to both the manufacturer and the operator of the switch is a question that would likely be answered in court.

At the other end of the spectrum, cyberterrorism and cyberespionage is clearly meant to inflict damage either on a company or on the general public. These types of attacks are particularly worrisome to investors who ultimately bear the burden of any financial repercussions as a result of these attacks.

While any entity that is connected to the internet is at risk of attack in cyberspace, from the investment communities viewpoint, we are particularly concerned about those companies, industries, and sectors which are critical to the national infrastructure: including telecommunications, electric power, water utilities, banking and financial institutions, oil and gas facilities, transportation, government services, and emergency services. The ability to disable or cripple any of these sectors, in our opinion, could have far-reaching economic implications beyond any individual company.

This is not meant to infer that those companies and industries that are not considered critical to the national infrastructure do not need to be just

as vigilant in their security systems. The consensus opinion from our analysts is that all industries and companies should be equally concerned about information technology security issues because it is an issue that has an enormous potential to negatively impact the valuation of a company's stock.

At a fundamental level, every business must be concerned with the security of its information technology systems. While everyone is aware of the threats, it must be the responsibility of corporate leaders to ensure that these threats are actually being addressed on an ongoing basis. At the same time, the investment community must keep the issue front and center of management. We will want to know what management systems are in place to assure that failures involving information technology will not critically endanger entire organizations or their partners. Furthermore, what are the systems and policies that assure accountability of your information technology security?

The ever increasing dependence on information technology systems to run the physical assets of businesses and manage the unending flow of individual bits and pieces of information that inundate managers on a daily basis, dictates that these systems operate reliably 24 by 7, three

hundred and sixty five days a year. Moreover, because more and more sensitive information is being stored in electronic form, the potential for misappropriation of data increases as businesses become more interconnected.

Of course, managements are cognizant of these issues and companies can implement security systems to lessen these threats, however, it is impossible to eliminate them 100%. The potential for sensitive information to be misappropriated must be carefully assessed by individual companies, because once the genie is out of the bottle, the damage to customer and investor confidence will be extremely difficult to rectify.

On the same note, firms must be alert to attempts to alter information on their networks such as press releases or other documents that may have a material impact on share price. A recent example occurred with two biotechnology companies in which a hacker was able to post false statements in which one company announced that it would be acquiring the other. On the news, both stocks opened up between 20% - 25%. Once the nature of the story was fully disseminated the stocks retraced their gains and ended down.

In the Amazon.com, Ebay and Yahoo cases mentioned earlier, their stock prices slide between and 17% -23% during the weeks that followed the attacks on their web sites. To put these losses in context, in a three-week period between February 8<sup>th</sup> and February 22<sup>nd</sup>, Ebay lost \$4.56 billion in market cap, Amazon lost \$6.67 billion and Yahoo lost \$17.24 billion. While the broader market (S&P500) was down about 6% over the same time period, in our opinion, investors punished these stocks in reaction to the company specific events surrounding the hacking incidents.

The rapid pace of technological advancement that has been one of the catalysts of the historic prosperity of the past two decades necessitates the continuous upgrading and maintenance of security systems to guarantee the integrity of our information technology infrastructure.

According to IDC, roughly \$5 billion was spent worldwide on Internet Security in 1999. This is only 0.5% of the \$834 billion dollars of total IT revenue in 1999. While we will reserve judgment on whether or not this represents an adequate level of security, we challenge each company to examine its own information technology security and answer three basic questions: what is our information technology infrastructure's exposure to attacks in cyberspace, what have we done to address these threats, and finally what is the potential economic impact if we are attacked and our systems fail; in terms of lost revenues dollars, but more importantly, in terms of lost customer and investor confidence and relationships. In today's volatile markets where information literally moves at the speed of light and investors shoot first and ask questions later, businesses can ill afford to be laggards in information technology security.

###